

## Executive Summary

Our medical system is changing, with choices to be made by consumers, providers, insurers, purchasers, and policy makers at every level of government. The need for quality improvement and for cost saving are driving both individual choices and health system dynamics. However, no one at any level can make these choices wisely without research showing the pros and cons of alternatives in health services. This information comes from data on the outcomes that individuals or organizations experienced with a particular input—the selection of a health plan, drug, or health care delivery model. Yet these same data are information (often personally identifiable health information) about individuals. Most individuals value their privacy and, when they have chosen to share personal information with a health care provider, are then justifiably concerned about possible breaches in the confidential handling of that information. The health services research that we need to support informed choices depends on access to data, but at the same time, individual privacy and patient–health care provider confidentiality must be protected.

### **HEALTH SERVICES RESEARCH AND QUALITY ASSURANCE OR IMPROVEMENT**

Health services research (HSR) is the study of the effects of using different modes of organization, delivery and financing for health care services. More precisely, a recent Institute of Medicine (IOM) publication explained, “Health services research is a multidisciplinary field of inquiry, both basic and applied, that examines the use, costs, quality, accessibility, delivery, organization, financing, and outcomes of health care services to increase knowledge and understanding of the structure, processes, and effects of health services for individuals and populations” (IOM, 1995). HSR includes studies of the effectiveness of health care interventions in real-world settings, as contrasted with studies of the efficacy<sup>1</sup> of interventions (e.g., new drugs) under controlled settings such as a clinical trial.

---

<sup>1</sup>The term “efficacy” refers to how reliably an intervention brings about a given result under ideal, controlled conditions. The term “effectiveness” refers to how an intervention performs in the complex and variable context of real-world use and practice.

### **BOX 1 Who Is the Intended Audience of this Report?**

This report is for all types of professionals and organizations that use or disclose data on health services. Although the Department of Health and Human Services is highlighted, the report should apply as well to other federal departments and agencies that are involved in human subjects research.

For organizations that have institutional review boards (IRBs) and whose research is subject to federal regulation:

- The practices and recommendations highlight some practices already in place in some IRBs and suggest additional support for IRB activities.

For organizations that use or disclose data but do not have an IRB or whose work is not subject to federal regulation:

- The practices and recommendations emphasize that human subjects protection from risks, including nonphysical risks from use of data, are of concern to anyone who uses or discloses data.

Although not all organizations have IRBs, all human subjects should be treated with the same high standards. The committee urges organizations that do not have IRBs to adopt practices of reviewing proposed investigations to assure that data confidentiality will be maintained. The committee likewise urges organizations that have, as well as those that do not have, IRBs to adopt system-wide confidentiality procedures and policies to protect nonresearch and research data.

As an applied field of study, HSR is closely related to nonresearch investigations that are directed toward assessing and improving the quality of operations in healthcare organizations. Indeed, HSR and health care operations form two ends of a continuous spectrum. Some HSR projects are clear examples of research; applying scientific methods to test hypotheses and produce new, generalizable knowledge. Other projects are certainly clear examples of internal exercises to assess the quality of the operations of the specific organization with no intention of producing generalizable knowledge. Many of these quality assessment or quality improvement (QA or QI) exercises are never intended to have any application beyond the specific unit within the organization that carries out the operation. In fact, many projects may start out as operations assessment and then become more like research, and many research projects involve doing very much what would be done in an internal operations assessment. As a result, for many projects, it is difficult to decide whether they are more like research, or more like QA or QI.

The benefits to society of HSR studies include increased understanding of the results of policy changes and other systemic effects of health care delivery systems. The major risks to subjects in HSR are not physical risks, such as unknown side effects of new drugs or invasive medical procedures, but psychosocial and financial risks resulting from improper disclosure of personally identifiable health information from the databases. That is, the potential for harm comes about through possible breaches of confidentiality in handling private and identifiable health information. Examples of the kinds of psychosocial or financial risks that may occur in-

clude potential denial of health insurance coverage, difficulty obtaining employment, embarrassment, loss of reputation, legal liability, or anxiety about what the recipient of an unauthorized disclosure of information might do with it.

The protection of privacy is a fundamental value in our culture. Research leading to improvements in the delivery and outcomes of health care, however, may be possible only with analysis of databases containing personally identifiable health information. Privacy can be protected by limiting access to data, or properly de-identifying the data, and by establishing other strong safeguards to ensure confidentiality. HSR can be only conducted if researchers have access to data, so it is important to concentrate on de-identification and other safeguards. We must protect both individual privacy and the societal benefits of research in order to achieve the appropriate balance. This report aims to highlight some practices that protect privacy while allowing research access to data.

## PROTECTION OF HUMAN SUBJECTS

The involvement of living human beings in research as subjects is governed by federal regulations when the research is federally supported or otherwise subject to federal oversight. The body of federal regulations about human subjects protection is called the *Common Rule*, since it has been adopted “in common” by many federal departments and agencies that conduct, support, or regulate research with human subjects. Each department or agency has codified the Common Rule in its own specific regulations; this report mainly uses the regulations for the Department of Health and Human Services (DHHS) are located at title 45 CFR part 46, subpart A for example.

The main mechanism for protecting research subjects and for assessing the balance of risks and benefits of research is the *institutional review board*, or IRB (specified in 45 CFR 46). An IRB is a standing committee composed of scientists, physicians, and others not directly involved with the proposal being reviewed (The IRB’s membership and function are defined in the regulations to ensure that it has sufficient expertise and diversity to provide appropriate review. Diversity should include gender, race, culture, and profession. In addition to scientists, the IRB must include at least one person who is not otherwise connected with the institution and at least one non-scientist.). IRBs review proposals for research on humans to make sure that risks to subjects are minimized, that the potential benefits of the research outweigh the risks to subjects, and that the subjects will be respected as persons and not just used as research subjects. Under federal regulations, IRBs are required to ensure that subjects first be fully informed of the risks and benefits of the research and then have an opportunity to consent or decline to participate in the research unless the IRB decides that consent can be waived.

When an institution receives federal funds to conduct research involving human subjects, the institution must promise the government that it will operate an IRB according to federal research regulations for that research. Privately funded research that will be submitted to federal regulatory agencies, such as the Food and Drug Administration (FDA), must also be approved by an IRB that complies with federal regulations for the protection of human subjects. These regulations specify that in order to approve research, the IRB must be satisfied that among other requirements (45 CFR 46.111),

- risks to subjects are minimized and are reasonable in relation to anticipated benefits,
- selection of subjects is equitable,
- informed consent is obtained to the extent required, and

- provisions to protect the privacy of subjects and to maintain the confidentiality of data are adequate.

IRBs face complicated decisions when reviewing HSR and deciding whether such research is eligible for a waiver of informed consent. HSR protocols often have characteristics, such as the absence of any physical risk to subjects, that may make them eligible for a waiver of the informed consent requirement or even for exemption from IRB review. Because many HSR projects depend on secondary analysis of databases of records previously collected for another purpose, the investigator may not have the ability to contact the original subjects, and even if locating them is theoretically possible, the number of individuals in question may be far too large to make contacting them practicable. Indeed, many HSR projects could not be carried out if consent were required. In such situations, an IRB may grant the investigator a waiver of informed consent. Yet, when the IRB reviews HSR, it must make sure that confidentiality risks are not overlooked. Finally, private organizations do their own HSR or have programs such as quality improvement that use similar data and methods; this research may not be covered by the federal regulations and these organizations sometimes do not have IRBs.

The committee supports the review of all HSR proposals by knowledgeable individuals who are independent of the researchers. Although not all HSR is subject to federal regulations, the committee also concluded that the review of HSR ought to follow the principles of these regulations. Such a review body might be designated by any of several titles. The term “IRB” is defined in federal regulations and therefore has implications of the extension of federal oversight in a new area. The term “privacy board” has been used in a rule that, as this report was being written, had been proposed but not finalized, and it may mean different things to different people. Throughout the report the committee has used the term “IRB” to refer to formally chartered review bodies that are required to follow the Common Rule and other federal regulations. The term “IRB or other review board” is used to refer to bodies that review research but are not necessarily required to follow these federal regulations, although the committee urges them to follow voluntarily the ethical principles underlying the regulations.

## GOOD PRACTICES

The objective of this project was to collect, to the extent possible, from workshop participants and other contributors, current best practices that IRBs and other review bodies employ to review research proposals and to ensure that privacy and confidentiality will be maintained within a balance between risk and benefit. Good IRB practices should apply the principles of ethical human subjects research and also be feasible for the type of research and the type of organization in question. That is to say, if we agree that we want to support HSR and obtain the societal benefits of research, then we must identify and implement practices that are feasible but that adequately protect the subjects. The committee hopes that the practices highlighted in the following chapters will facilitate HSR with appropriate and feasible mechanisms for the protection of human subjects, and will stimulate the development and dissemination of more advanced practices in the future.

In highlighting the empirical collection of practices, the committee recognized that good principles are already codified in the federal regulations on human subjects protection, but that no amount of codification can provide adequate direction for the day-to-day, study-by-study, work of an IRB. In short, regulations and guidelines are important to provide norms, but they

must still be implemented with the judgment and practical experience of individuals closest to the situation. This is what the local IRB system is designed to do. The sense of the committee is that the local IRB system is strong and fully capable of reviewing HSR for privacy and confidentiality issues. Any IRB or other review body that reviews HSR will, however, have to understand the special problems of HSR and how to apply the principles embodied in the federal regulations. The aim of sharing best practices is to support review bodies by compiling the good ideas that have already been developed by IRBs and put into practice. One challenge of the future will be to find the best means of disseminating these good ideas.

## PROJECT AND SCOPE

The IOM Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protection was formed in December 1999 to gather data on the current and best practices of IRBs in protecting privacy (complete charge is given below). Two DHHS agencies, the Agency for Healthcare Research and Quality (AHRQ) and the Office of the Assistant Secretary for Planning and Evaluation (ASPE), sponsored the project.

To address these tasks, the IOM assembled a 12-member committee with expertise in medical ethics, HSR, IRB function, statistics, computer science, law, and database management. The committee met by telephone conference in January 2000. The committee and the IOM then convened a public workshop in March 2000. The committee invited testimony from IRB chairs and administrators, health services researchers, and other officers of academia, government, and private industry (see Appendix B). The workshop also featured presentations of the drafts of two commissioned papers, one addressing special considerations of HSR and confidentiality when the data pertain to minors (see Appendix C) and the other presenting an international comparison of health information privacy standards (see Appendix D). In addition to the workshop, the committee posted an invitation on a list serve and on the National Academies' website to IRBs to contribute information (see Appendix A). The committee collected further information informally by e-mail and telephone. Although the committee received just a few responses to the posted call for information, those received were very informative. The committee noted that all the providers of information, including respondents to the call for information, those who briefed the staff by telephone, and participants in the workshop, are a self-selected group of professionals committed to the IRB process. Information collection was thus not systematic and random, but particularly targeted. The committee deliberated by telephone and e-mail, and in closed meetings in April and May 2000, about the practices described to it. Finally, the committee has summarized in this report the practices it heard that seemed to be most effective. The committee addresses privacy and confidentiality pertaining to data used for HSR conducted through analyses of preexisting databases. There are many other aspects of the privacy of electronic medical records that were beyond the charge of the committee. The information in this report however—its findings and recommendations—applies as well both to data previously collected for another purpose and now being secondarily analyzed and to data derived in other ways. The committee chose to focus its work on studies involving analyses of data already collected for other purposes because such studies pose the most difficult ethical issues regarding HSR. Although HSR that utilizes surveys and interviews also raises ethical issues, the contact between researchers and subjects allows the subjects to learn about the research and decline to participate if they so choose. The committee recognized the strong connections between these related matters and the question of protecting data privacy in HSR using existing data. The committee therefore asks

readers to bear in mind that such related matters were not in its charge and the committee did not address them.

The purpose of this project was to provide information and advice to the sponsors on the current and best practices of IRBs in protecting privacy in health services research. The charge to the committee was given in three parts as shown below.

1. To gather information on the current practices and principles followed by institutional review boards to safeguard the confidentiality of personally identifiable health information used for health services research purposes, in particular, to identify those IRB practices that are superior in protecting the privacy, confidentiality, and security of personally identifiable health information.

2. To gather information on the current practices and principles employed in privately funded health services research studies (that are generally not subject to IRB approval) to safeguard the confidentiality of personally identifiable health information, and to consider whether and how IRB best practices in this regard might be applied to such privately sponsored studies.

3. If appropriate, to recommend a set of best practices for safeguarding the confidentiality of personally identifiable health information that might be voluntarily applied to health services research projects by IRBs and private sponsors.

## RECOMMENDATIONS

This section presents the committee's recommendations and findings based on the available information from IRBs working under federal regulations, discussed in more detail in Chapter 3, as well as recommendations from Chapter 4, on public and private health care companies that may not have IRBs or be subject to federal regulation. Chapter 5 suggests some directions for further work.

### Best Practices for IRB Review of HSR Subject to Federal Regulations (Chapter 3)

**Recommendation 3-1. Organizations should work with their IRBs to develop specific guidance and examples on how to interpret key terms in the federal regulations pertinent to the use in HSR of data previously collected for other purposes. Such terms include *generalizable knowledge*, *identifiable information*, *minimal risk*, and *privacy and confidentiality*. Organizations and their IRBs should then make such guidance and examples available to all investigators submitting proposals for review.**

The committee found that several topics cause considerable worry to investigators and IRBs because federal regulations are open to varying interpretations, with divergent implications.

- The first of these topics is what activities are considered research and what criteria are used to operationalize the distinction between research and other activities. A key feature of the federal definition of research is whether the activity contributes to generalizable knowledge. In trying to distinguish research from activities such as quality improvement that use similar techniques to analyze personally identifiable health information in databases, however, both the fed-

eral regulations and the interpretations of these regulations by the Office of Human Research Protections (OHRP, formerly the Office for Protection from Research Risks, or OPRR) contain insufficient practical guidance for investigators and IRBs.

## **BOX 2 Highlights of the Recommendations**

*Institutional review boards should:*

- Help develop, and make accessible to investigators, materials including specific guidance and examples showing the implementation and interpretation of federal regulations, points to consider regarding protecting privacy and confidentiality in HSR, and review forms specifically designed for HSR (3-1 to 3-3).
- Educate themselves about the specific features and methods of HSR, and recruit or retain expertise (either on the committee or through consultants) on confidentiality and security in HSR involving analysis of data previously collected for other purposes, including the risks of identification of individuals and the physical security of data (recommendations 3-3 to 3-5).
- Adopt the best practices of IRBs working under federal regulations, and apply these practices to the review of HSR that is not subject to federal regulation (recommendations 4-2 and 5-7).

*Health services researchers should:*

- Have all HSR reviewed by an IRB or other review board with sufficient expertise in privacy or confidentiality protection, regardless of funding source or whether the institution is required to have all research conducted under federal regulation (4-1).
- Educate themselves to be aware of the best available techniques for confidentiality protection, including being careful to collect and retain only those fields that are truly needed (recommendations 3-5).
- Voluntarily adopt and/or support the use of best practices for the review of HSR by IRBs or data privacy boards (5-9).

*Institutions funding, sponsoring or publishing research should:*

- Promote education for members of the IRB or other review board regarding the special issues of research using health information previously collected for some other use and its impact on the protection of the privacy and confidentiality of human subjects (3-5).
- Have comprehensive policies, procedures, sanctions, and structures to protect health data confidentiality throughout the organization when personally identifiable health information is used for research or other purposes (4-3 and 4-4).
- Ensure adequate administrative support and funding for their IRBs or other review boards and incorporate improvement of IRB operations into overall institutional strategic planning (5-1).
- Voluntarily adopt and/or support the use of best practices for the review of HSR by IRBs or other review boards (5-9).
- Have all HSR reviewed by an IRB or other review board regardless of funding source or whether the institutions hosting the research or providing the data have agreed to carry out all research under federal regulations (4-1).

*Continued*

**BOX 2 Continued****The federal government Department Health and Human Services should:**

- Provide more specific guidance to IRBs, clarifying the range of discretion that local IRBs have to interpret federal regulations and continue or expand educational efforts, along with private organizations committed to HSR such as the American Association of Medical Colleges, Association for Health Services Research (now the Academy for Health Services Research and Health Policy), American College of Epidemiology, International Society for Pharmacoepidemiology, Professional Responsibility in Medicine and Research, and Applied Research Ethics National Association (5-2).
- Continue and expand efforts to encourage holders of personally identifiable health information to make this information available to researchers as public use files after suitable application of techniques to minimize the risks of identifiability, and ensure that the data provided for HSR use are prepared in a manner that protects confidentiality adequately, including covering the cost of preparing government-held personally identifiable health information, so that confidentiality can be adequately protected in HSR (5-3 to 5-5).
- Consider supporting studies on the feasibility of developing procedures for facilitating linkage of separate data files containing sensitive data from different sources to create analytical files that are anonymized or for which the probability of identifying subjects is low, and on the extent to which IRBs assess nonphysical risks to human subjects (5-6 and 5-7).
- Consider other changes in policy and procedure including changing regulatory reference to “exempt” and “expedite” in the case of HSR to “administrative review” (5-8).

- A second important issue is what constitutes identifiable information as defined in the federal regulations. Should data be considered unidentifiable if linked to codes in such a way that the investigator would have great difficulty reestablishing the identity of subjects?

- A third issue is what constitutes minimal risk in HSR research and, in particular, what steps to protect confidentiality of data in HSR suffice to allow the project to be considered as minimal risk. The issues of identifiable information and minimal risk have important implications for whether a project may be exempt from IRB review or receive expedited review or whether informed consent of research participants may be waived. The committee felt that it would be desirable that all such research proposals receive some outside review.

On all of these issues, IRBs should communicate more directly with investigators and give examples more specific than the guidance currently available in federal regulations and clarifications by OHRP. Clearer guidance would make IRB review more efficient as well as enhance the protection of subjects by helping to ensure that HSR projects incorporate confidentiality protections that the reviewers find important.

**Recommendation 3-2. IRBs should develop and disseminate principles, policies, and best practices for investigators regarding privacy and confidentiality issues in HSR that makes use of personal health data previously collected for other uses.**

Confidentiality in handling health information is important for its own sake and for the enhancement of public trust in research. The committee heard several innovative and feasible ways to facilitate the maintenance of confidentiality. The committee found, however, that the possible



identifiability of data in HSR is a continuum, such that absolute guarantees of confidentiality are impossible.

Many techniques work together to increase the safety of confidential data, including protecting the data from unauthorized access by tracking who reviews the file, storing identifying information or codes separately from the rest of the data, and protecting the data from being physically lost, stolen, or surreptitiously copied.

**Recommendation 3-3. IRBs should redesign applications and forms (paper and electronic) tailored to HSR that analyzes data originally collected for other purposes and then distribute them widely (e.g., post them on-line) to assist investigators in writing the human subjects sections of their HSR proposals and in preparing applications for IRB review. IRBs should be knowledgeable about the differences between HSR and clinical research, and any forms developed should reflect these differences.**

A checklist or logical series of questions lays out the criteria that the institution has adopted to determine, for example, what constitutes research. These instruments are useful in several ways: they call the attention of investigators to ethical issues arising in HSR, and they help investigators to think through systematically the specific issues regarding IRB review, patient consent, and protection confidentiality. Here, for example, is one approach to classifying a project along the HSR to QA–QI spectrum:

The following are characteristics of projects using HSR methods that are research, not QA or QI:

- It explores previously unknown phenomena.
- It collects information beyond that routinely collected for the patient care in question.
- It compares alternative treatments, interventions, or processes.
- It manipulates a current process.
- The results are expected to be published for general societal benefit.

**Recommendation 3-4. IRBs should have expertise available (either on the committee or through consultants) to evaluate the risks to confidentiality and security in HSR involving data previously collected for some other purpose, including the risks of identification of individuals and the physical and electronic security of data.**

Many of the techniques mentioned can be highly technical and are evolving rapidly. In order to confirm that confidentiality will be protected in a protocol, the reviewers will have to have access either to members or to consultants who can advise them on whether the proposal includes feasible technical measures to protect the data or whether the proposal has overlooked some potential confidentiality risks. This training should include cross-cultural issues related to definitions of privacy of personal, family and group information, depending on the specifics of how such cross-cultural questions arise in the local situation.

**Recommendation 3-5. Institutions that carry out HSR and train health services researchers should require that trainees, investigators, and IRB members receive education, with updates as technology changes, regarding protection of privacy and confidentiality when using data previously collected for another use.**

Education is critical not only for IRB members, but also for researchers, technicians, and any other employees who may come into contact with personally identifiable health information. Better education about how to protect confidentiality and possible sources of risk will help investigators design better confidentiality protection for their proposed studies from the start. Better education of all employees who may come in contact with the data will help raise the level of understanding and alertness throughout the organization.

**Recommendation 3-6. Health care or other organizations that disclose or use personally identifiable health information for any purpose including research or other activities using HSR methods should have comprehensive policies, procedures and other structures to protect the confidentiality of health information and should have in place appropriate strong and enforceable sanctions against breaches of health information confidentiality.**

Access to specific expertise and enhanced general education are important, but the committee also observed that the human element of the research enterprise necessarily includes human potential for error and even malfeasance. Therefore organizations should complement and support the proactive strategies of expertise and education for better confidentiality protection with deterrents to wrongdoing. Such sanctions should be graded according to the offense (e.g., whether the incident was a simple mistake or intentional violation) and should apply not only to researchers but to all employees of the organization.

#### **Best Practices for Review of HSR Not Necessarily Subject to Federal Regulation (Chapter 4)**

A good deal of health services research is carried out by organizations that do not receive federal funds for research and are not subject to federal regulations. These same organizations are dedicated to delivering health care services and products, so they also engage in quality assessment and quality improvement projects. These activities may involve very similar methods and uses of data, but they may not be classified as research.

The committee was impressed with the commitment to privacy and confidentiality that the representatives of several private companies presented at the workshop. Companies appear to be at different stages of developing internal privacy or confidentiality policies regarding HSR and should be encouraged to continue to develop these organizational policies and procedures.

**Recommendation 4-1. Researchers should have all HSR reviewed by an IRB or other review board regardless of the source of support or whether the research is subject to pertinent federal regulations.**

**Recommendation 4-2. IRBs and other boards that review HSR that is not subject to federal regulation should assess their practices in comparison with the best practices of IRBs working under pertinent federal regulations and, when the latter offer improvements, adopt them. Alternatively, when their own practices are superior though not subject to federal regulation, they should share them with IRBs applying the Common Rule.**

IRBs offer a review of research projects by knowledgeable persons not directly associated with the project. This independent review protects subjects of research because independent reviewers may identify concerns and suggest ways to minimize risks that were not apparent to in-

investigators. The committee heard several examples of protocols that were or could have been substantially improved with respect to confidentiality by relatively simple modifications, for example, omitting identifying data in the record, such as a Social Security number, that was not actually necessary for the research. Research subjects, who undergo risks for the benefit of science and society as a whole, should have the protections of such independent review as a matter of ethical best practice, regardless of funding source. There is little ethical justification for making a distinction between the level of protection afforded subjects in federally funded projects and that given subjects in projects funded by private sources if the risks to these subjects are comparable.

As in Recommendation 3-2, IRBs or other review bodies should develop lists of points to consider on protecting privacy and confidentiality in HSR for use by investigators. As noted in Recommendation 3-3, the committee suggests that the development and on-line posting of applications and review forms specifically designed for HSR would improve the quality of review of HSR projects. IRBs and other review bodies in any setting should inform themselves about the differences between HSR and clinical research, and any forms developed should reflect these differences. As mentioned in Recommendation 3-4, IRBs or similar review bodies should have available expertise (either on the committee or through consultants) to evaluate the risks to confidentiality and security in HSR, including the risks of identification of individuals and the physical security of data. Also, as stated in Recommendation 3-5, organizations should require that researchers and other employees who come in contact with confidential health information receive education in the handling of this information to maintain confidentiality.

**Recommendation 4-3. Health care organizations that conduct projects applying the methods of HSR to personally identifiable health information for purposes such as QA or QI, disease management, and core business functions as well as for research should have comprehensive policies, procedures, and other structures to protect health privacy when personally identifiable health information is used for research or other purposes.**

**Recommendation 4-4. Health care or other organizations that disclose or use personally identifiable health information for any purpose including QA or QI, disease management, and core business functions as well as for research should have in place appropriate, strong, and enforceable sanctions against breaches of the confidentiality of health information.**

The members of the committee agreed that previous experience provides ample evidence that, although most investigators and staff are upstanding, there will always be a few who are subject to the temptation to misuse access to confidential information or who maintain records in an insecure manner. In fact, the committee felt that this aspect of human subjects protection may have been neglected and therefore recommends consideration of deterrent policies both for organizations working with IRBs under the Common Rule and for those that do not.

Large health care organizations reported that most violations of confidentiality occurred outside the research arena, in such areas as clinical care and business activities. This distribution is not surprising because most uses of personally identifiable health information are in these nonresearch areas. From the viewpoint of the patient, it does not matter whether a violation of confidentiality occurs in a research project or other activity because the risks of being harmed or wronged may be the same.

## Recommendations for Next Steps (Chapter 5)

“The end of this study will not be the end of studying [the issue of privacy and confidentiality in health services research],” said Dr. Michael Fitzmaurice of AHRQ, one of the sponsoring agencies, during the committee’s workshop. The committee appreciated that the charge of this particular study was focused and accordingly endeavored to stay strictly within the charge. In the course of the study, however, the committee found many important questions that would seem to be answerable in practical terms, although doing so would be far beyond the scope of this report. The present project has, however, brought these other issues into a new sharper focus. The committee’s suggestions for further work and future steps may communicate this vision to others.

**Recommendation 5-1. Institutions whose IRBs or other review boards review HSR should ensure adequate administrative support and funding for review bodies and should incorporate improving review operations into overall institutional strategic planning, and organizations that sponsor HSR should also support designating adequate funds for such review.**

The committee corroborated previous reports that questioned whether IRBs have the resources to carry out their mission. The committee noted especially the April 2000 update report of the DHHS Office of the Inspector General (OIG). This report, *Protecting Human Research Subjects: Status of Recommendations*, concluded that the resource problems identified in the OIG’s 1998 report, *Institutional Review Boards: A Time for Reform*, still exist. The committee heard that many IRBs already have a heavy workload of proposals for review, and that most members serve in a voluntary capacity. In addition, the practices that the committee heard and believes can be positive facilitators of IRB quality and efficiency in the review of HSR will require investment on the part of the IRB’s institutional home in computer equipment, applications development, and expertise to support these programs and advise the organization.

**Recommendation 5-2. The DHHS and other federal departments and private organizations such as the American Association of Medical Colleges, the Association for Health Services Research (now the Academy for Health Services Research and Health Policy), the American College of Epidemiology, the International Society for Pharmacoepidemiology, Professional Responsibility in Medicine and Research, the Applied Research Ethics National Association, and others should continue or expand educational efforts regarding the protection of the confidentiality of personally identifiable health information in research.**

While these recommendations highlight DHHS as the sponsor of this study and a major sponsor of relevant research, the recommendations should be applied by other Common Rule signatory departments and agencies as well. The committee believes that the approach of identifying best practices for IRB oversight of HSR is a fruitful one that should to be further developed. Recommendations of best practices will provide more specific guidance to investigators and IRB members than is currently available, and IRBs will continue to devise additional good practices. This approach draws its strength from the commitment both of IRB members and administrators and of researchers to protecting the rights and welfare of the subjects of HSR. Both IRBs and scientists have developed useful practices that, if more widely adopted, could lead to improved protection of confidentiality and privacy, without creating undue burdens.

**Recommendation 5-3. Organizations that furnish health services researchers with personally identifiable health information should ensure that the data are prepared in a manner that protects confidentiality adequately.**

The committee heard several instances reported at the workshop where HSR investigators requested de-identified data from federal agencies but received data that had not been de-identified because the agency in question lacked the resources to do so.

As large holders of personally identifiable data, federal agencies should not be in the situation of having to choose between providing data that have not been de-identified, or simply refusing to provide data for research at all. Organizations holding personally identifiable health data should develop and/or implement lists of points to consider in reviewing data requests with respect to protecting privacy and confidentiality in HSR.

**Recommendation 5-4. The funders of HSR should be willing to cover the cost of preparing personally identifiable health information that is collected in clinical care, billing, or payment so that confidentiality can be adequately protected in HSR.**

**Recommendation 5-5. The DHHS should continue and expand efforts to encourage holders of personally identifiable health information to make this information available to researchers as public use files after suitable application of techniques to minimize the risks of identifiability.**

If an organization holding health data has made a dataset publicly available without restriction, as is done with the National Health Interview Survey (NHIS), then projects using only such data can be considered minimal risk and eligible for exemption per 45 CFR 46.101(b)(5). In order to promote HSR, data-holding organizations should consider making as much data available in the public domain as is safely possible. The committee notes that the Interagency Confidentiality and Data Access Group (affiliated with the Federal Committee on Statistical Methodology) has developed a checklist for use in considering whether data may be released, which helps holders of data develop such public use files.<sup>1</sup>

**Recommendation 5-6. The AHRQ should consider supporting a feasibility study on developing procedures for facilitating linkage of separate data files containing sensitive data from different sources to create analytical files such that it would be possible for researchers to create linkages that are reliable and informative, and at the same time, to protect the confidentiality of the original data disclosure through de-identification and other protective measures so as to save the subject from being placed at risk of harm or wrong through improper re-identification.**

Much of the value of retrospective, database-oriented research comes from the ability to draw inferences from data derived from different sources. The committee urges interested parties, including DHHS agencies, to encourage research on linkage and anonymization with a view toward two goals: first, it should be possible for researchers to create linkages that are reliable and informative, and second, we should approach as closely as possible the goal of anonymized data. Ideally then, the various sources of data would have their records indexed by the same set of identifiers, but ones that are not easily reassociated with the actual patient's identity. There are several possible ways to address this problem. One suggestion exploits developing cryptographic and authentication technology to create flexible health information identification systems (as explored in a pilot study of Kohane et al., 1998). Another type of linkage system would depend on

---

<sup>1</sup>Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology. Checklist on Disclosure Potential of Proposed Data Releases (July 1999): <http://www.fcsm.gov/spwptbco.html>.

trusted third parties with no interest in either data collection or the research project to be responsible for linking the separate data files. These entities could hold the keys linking individuals to the data. After merging datasets, this entity would then strip off the identifiers, check that identification cannot be (reasonably) inferred<sup>2</sup>, and take any needed steps to protect the data. There are positive and negative aspects to either approach, so the feasibility of both should be further tested.

**Recommendation 5-7. DHHS (AHRQ and/or the NIH) should consider developing and supporting a research agenda concerning IRB protection of subjects from nonphysical harms such as risks to privacy and confidentiality in human subjects research (including cultural meanings of privacy and confidentiality).**

A systematic study of nonphysical risk assessment was beyond the charge given to this IOM committee, and the committee would in any case have found itself unable to accomplish it due to time limitations and rules of the Office of Management and Budget requiring additional clearance for extensive surveys. The committee found, however, that such information would be of great use both as a baseline and, if updated periodically, as a basis of continuous policy evaluation. Such a research agenda would likely include current IRB practice as well as new procedures and policies to provide better human subjects protection and also would include monitoring of IRB practices. The findings would be of use to IRBs, researchers, regulators, and any other parties interested in privacy and confidentiality.

**Recommendation 5-8. The OHRP should consider proposing a change to the regulations with respect to HSR to replace the terms “exempt” and “expedite” with “administrative review.”**

The committee is recommending this only with respect to HSR, not having investigated possible consequences for other types of research. The committee heard several reports that well-intentioned and conscientious researchers may judge a study to be exempt from review under the current regulatory language and therefore never bring it to the attention of a review board. Since the committee has concluded that all HSR should receive some review by a board that is independent of the research project, the committee suggests that this possibly misleading terminology be avoided. The committee recognizes, however, that a change to the Common Rule involves coordination among many agencies. The committee further recognizes that others may have other suggestions for a new term. The committee’s goal in this matter was to offer a term that recognized that some studies do not need full IRB review but does not seem to suggest that the investigator should decide what level of IRB review is needed.

**Recommendation 5-9. Health services researchers, and institutions that participate in and benefit from HSR, should voluntarily adopt best practices for IRB review of HSR.**

The committee found that some nations have adopted laws or regulations that allow individuals to exclude their personally identifiable health information from databases, that require written consent from patients for use of health records for research, and that require the anony-

---

<sup>2</sup>The committee recognizes that the question of how difficult identifiability by inference must be in order to make data safe for release will continue to be a matter of debate and notes that the standard should be expected to change as technology changes.

mization of data for use in any secondary data analysis. Such measures were enacted to protect privacy and the confidentiality of computerized personally identifiable health information.

If patients and members of the public in general do not find that they can trust that confidential information will be protected throughout research, they may seek further measures to protect confidentiality that could be detrimental to HSR. The committee therefore urges investigators, data users, and data holders and publishers voluntarily to adopt and continually upgrade the best practices of IRBs and other review boards in ensuring the protection of data privacy and confidentiality in HSR.

**Recommendation 5-10. All stakeholders in HSR should support strategies to improve the protection of privacy and confidentiality without impeding research.**

The committee found it necessary to at least contemplate additional areas for study. Although there was not time in this project to explore wider- ranging ideas, the committee suggests several as potential starting points in a multifaceted strategy to improve the awareness of privacy issues and improve confidentiality protection practices.

- Federal departments including the DHHS could sponsor a conference to include HSR journal editors and editorial boards to consider special issues devoted to data privacy and adoption or strengthening of policies against publishing research without evidence of prior assessment by an IRB or other review board.

- DHHS and other federal departments and agencies, as well as foundations and state and local granting agencies, could consider possible changes in procedure including revising grant application guidelines and contract proposals to include a section on confidentiality protection and to include privacy experts on peer review panels.

- Funders of HSR including DHHS or other federal departments, foundations, accrediting agencies, health maintenance organizations and private companies could consider supporting research on data protection methods.

- Organizations interested in data privacy and high-quality HSR could sponsor a prize competition for best practices in protecting privacy and confidentiality.

The methods of HSR, applied to data previously collected for other purposes, have been useful in discovering and demonstrating systemic effects and population-level trends in the organization and delivery of health services. It is important that we, as a society, continue to have access to such research in order to inform policy making in both private and governmental arenas. At the same time, it is important that we, as a society, protect the privacy of individuals and of vulnerable groups, and the confidentiality of information that patients share with health care providers. As a result of the present study, the committee has concluded that it is possible both to carry out valuable HSR and to protect confidentiality. However, to do so will require adequate funding. Resources are needed to support dedicated, trained IRB members and staff, to establish organizational confidentiality policies and electronic security practices, to educate researchers, and to provide statistical and computer expertise. The true test of our commitment to the twin values of advancing useful knowledge and protecting confidentiality is whether we are willing to make the needed investments to achieve both goals.